EPSON
EXCEED YOUR VISION

Administrator's Guide

Contents

Administrator's Guide **7**

Using Web Config Network Configuration Software **8**

About Web Config 8

Accessing Web Config 8

Restricting Features Available for Users 9

User Feature Restriction 10

Configuring User Feature Restrictions 10

Changing the Administrator Password in Web Config 12

Using Your Product on a Secure Network 13

Configuring SSL/TLS Communication 13

Configuring SSL/TLS Settings 13

Configuring a Server Certificate for the Product 14

Configuring IPsec/IP Filtering 15

About IPsec/IP Filtering 16

Configuring Default IPsec/IP Filtering Policy 16

Configuring Group IPsec/IP Filtering Policies 17

IPsec/IP Filtering Policy Settings 18

IPsec/IP Filtering Configuration Examples 22

Configuring an IPsec/IP Filtering Certificate 23

Configuring SNMPv3 Protocol Settings 24

SNMPv3 Settings 25

Connecting the Product to an IEEE802.1X Network 26

Configuring an IEEE802.1X Network 26

IEEE802.1X Network Settings 27

Configuring a Certificate for an IEEE802.1X Network 28

IEEE802.1X Network Status 29

Using a Digital Certificate 30

About Digital Certification 30

Obtaining and Importing a CA-signed Certificate 31

CSR Setup Settings 33

CSR Import Settings 33
Deleting a CA-signed Certificate 34
Updating a Self-signed Certificate 34
Using an LDAP Server 35
Configuring the LDAP Server and Selecting Search Settings 35
LDAP Server Settings 37
LDAP Search Settings 38
Checking the LDAP Server Connection 38
LDAP Connection Report Messages 39
Using an Email Server 39
Configuring an Email Server 40
Email Server Settings 40
Checking the Email Server Connection 41
Email Server Connection Report Messages 41
Configuring Email Notification 42
Using EpsonNet Config Network Configuration Software 44
Installing EpsonNet Config 44
Configuring a Product IP Address Using EpsonNet Config - Ethernet 44
Configuring a Product IP Address Using EpsonNet Config - WiFi 45
Solving Problems 48
Solving Network Software Usage Problems 48
Cannot Find Access Web Config 48
The "Out of Date" Message Appears 49
"The name of the security certificate does not match" Message Appears 49
Model Name or IP Address Not Displayed in EpsonNet Config 49
Solving Network Security Problems 49
Pre-Shared Key was Forgotten 50
Cannot Communicate with the Product Using IPsec Communication 50
Communication was Working, but Stopped 50
Cannot Create the Secure IPP Printing Port 51
Cannot Access the Product After Configuring IEEE802.1X 51
Solving Digital Certificate Problems 51
Digital Certificate Warning Messages 51

Cannot Import a Digital Certificate 53
Cannot Update a Certificate or Create a CSR 53
Deleted a CA-signed Certificate 53
Where to Get Help 54
Notices 55
Trademarks 55
Copyright Notice 55
Copyright Attribution 56

Administrator's Guide

Welcome to the *Administrator's Guide*.

For a printable PDF copy of this guide, click here.

Note: Not all features mentioned in this *Administrator's Guide* are available with every product model.

Using Web Config Network Configuration Software

Follow the instructions in these sections to configure your product's adminstrator network settings using the Web Config software.

Note: Before you can configure system administration settings, connect the product to a network. See the product's *Start Here* sheet and *User's Guide* for instructions.

About Web Config
Accessing Web Config
Restricting Features Available for Users
Using Your Product on a Secure Network

About Web Config

Web Config is a browser-based application you can use to configure a product's settings. Basic and advanced setting pages are available.

Note: Before you can configure system administration settings, connect the product to a network. See the product's *Start Here* sheet and *User's Guide* for instructions.

You can lock the settings you select by setting up an administrator password for your product. See the product's *User's Guide* for instructions.

Parent topic: Using Web Config Network Configuration Software

Accessing Web Config

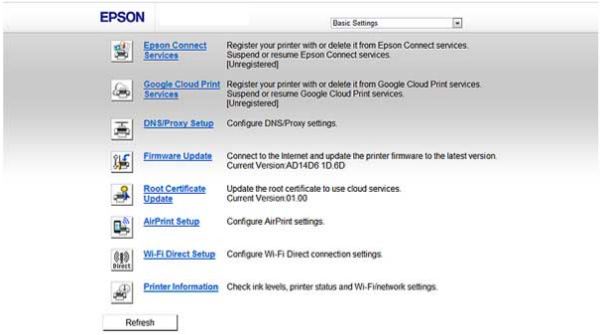
You can access Web Config from your browser using HTTP or HTTPS.

By default, you access Web Config for the first time using HTTP. If you continue to use HTTP, Web Config does not display all available menus.

1. Print a network status sheet for your product and identify the product IP address. See the product's *User's Guide* for instructions.
2. Start your web browser and make sure JavaScript is enabled.
3. Type the product IP address into the browser as follows, depending on the protocol you are using:
   - IPv4: http://*product IP address*

- IPv6: http://[*product IP address*]/

The Basic Settings page appears:


EPSON
Basic Settings
Epson Connect Services
Register your printer with or delete it from Epson Connect services.
Suspend or resume Epson Connect services.
[Unregistered]
Google Cloud Print Services
Register your printer with or delete it from Google Cloud Print services.
Suspend or resume Google Cloud Print services.
[Unregistered]
DNS/Proxy Setup
Configure DNS/Proxy settings.
Firmware Update
Connect to the Internet and update the printer firmware to the latest version.
Current Version:AD14D6 1D.6D
Root Certificate Update
Update the root certificate to use cloud services.
Current Version:01.00
AirPrint Setup
Configure AirPrint settings.
Wi-Fi Direct Setup
Configure Wi-Fi Direct connection settings.
Printer Information
Check ink levels, printer status and Wi-Fi/network settings.
Refresh

4. To use HTTPS, configure the address to use HTTPS in your browser.

   A message warning about the self-signed certificate appears.

To access Web Config after configuring the address to use HTTPS, enter https:// before the product IP address, shown in step 3.

Note: If the product name is registered with the DNS server, you can use the product name instead of the product IP address to access Web Config.

Parent topic: Using Web Config Network Configuration Software

Restricting Features Available for Users

Follow the instructions in these sections to restrict users from using certain product features and create an administrator password to lock the restrictions using the Web Config software.

User Feature Restriction

Configuring User Feature Restrictions

Changing the Administrator Password in Web Config

Parent topic: Using Web Config Network Configuration Software

User Feature Restriction

You can restrict available product features for up to 10 individual users, with different features available to each user. This requires users to log into the product control panel with their user name and password before they can use control panel features.

With Windows, you can also restrict printing and scanning from the product software. This requires users to log into the printing or scanning software, and allows the software to authenticate the users before printing or scanning proceeds. For instructions on setting up software restrictions, see the help utility in the printing or scanning software.

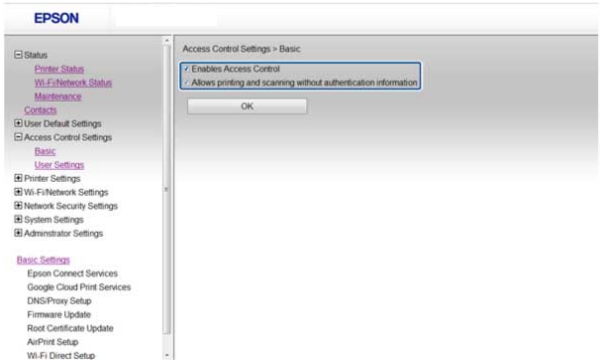
Parent topic: Restricting Features Available for Users

Configuring User Feature Restrictions

You can create up to 10 user accounts and restrict access to control panel features separately for each one.

1. Access Web Config, select **Access Control Settings**, and select **Basic**.

   You see a window like this:

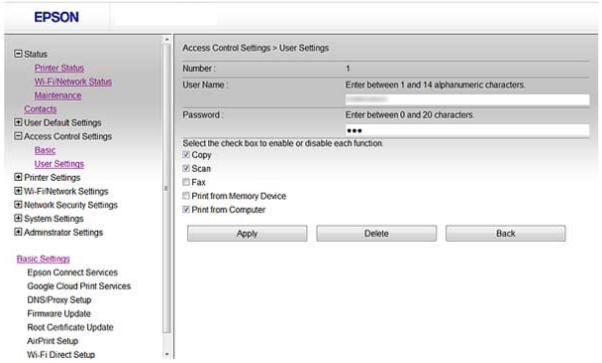


2. Select the **Enables Access Controls** checkbox.
3. If you have configured the product for an LDAP server or IEEE802.1x network, you can deselect the **Allows printing and scanning without authentication information** checkbox to prevent the product from receiving jobs sent from these sources:
   - The default operating system driver
   - A PCL or PostScript printer driver

- Web services such as Epson Connect or Google Cloud Print
- Smartphones and other mobile devices

4. Click **OK**.
5. Select **Access Control Settings** and select **User Settings**.
6. Click **Add**.

   You see a window like this:



7. Enter a name for a user in the User Name field following the guidelines on the screen. Use ASCII (0x20-0x7E) characters.
8. Enter a password for the user in the Password field following the guidelines on the screen.

   Note: If you need to reset a password, leave the password field blank.

9. Select the checkbox for each function you want the user to be able to perform, and deselect the checkbox for each function you want to restrict access to.
10. Click **Apply**.

    Note: When you edit a completed user account, you see a **Delete** option. Click it to delete a user, if necessary.

Note: You can import and export a list of user features using EpsonNet Config. See the help utility in the software for instructions.

Parent topic: Restricting Features Available for Users

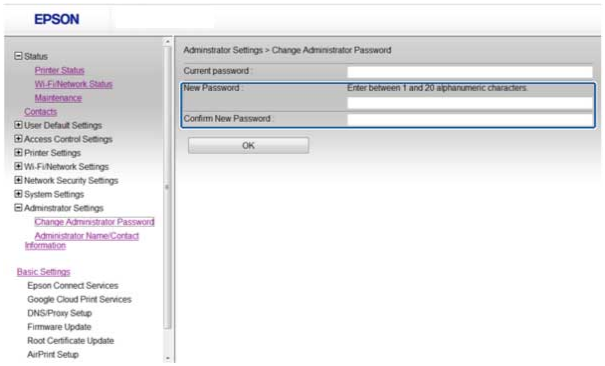
Changing the Administrator Password in Web Config

You can set an administrator password using your product's control panel or using Web Config or EpsonNet Config. You use the same administrator password in all cases.

Note: See your product's *User's Guide* for instructions on setting an administrator password using the control panel. If you forget your administrator password, contact Epson for support, as described in the product's *User's Guide*.

1. Access Web Config, select **Administrator Settings**, and select **Change Administrator Password**.

   You see a window like this:



2. Do one of the following:
   - If you have set an administrator password before, enter the current password, then enter and confirm the new password in the fields provided.
   - If you have not set an administrator password before, enter a new password and confirm it in the fields provided
3. Click **OK**

Parent topic: Restricting Features Available for Users

Using Your Product on a Secure Network

Follow the instructions in these sections to configure security features for your product on the network using the Web Config software.

Configuring SSL/TLS Communication
Configuring IPsec/IP Filtering
Configuring SNMPv3 Protocol Settings
Connecting the Product to an IEEE802.1X Network
Using a Digital Certificate
Using an LDAP Server
Using an Email Server

Parent topic: Using Web Config Network Configuration Software

Configuring SSL/TLS Communication

Follow the instructions in these sections to configure SSL/TLS communication using Web Config.

Configuring SSL/TLS Settings
Configuring a Server Certificate for the Product

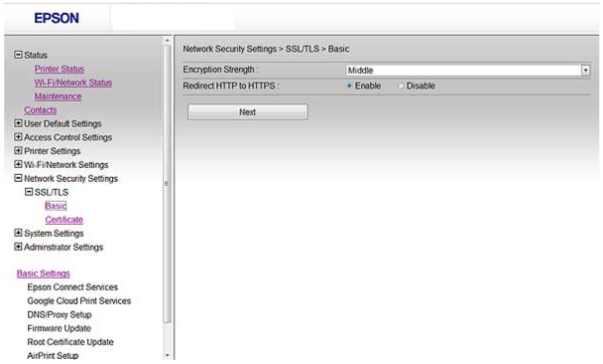
Parent topic: Using Your Product on a Secure Network

Configuring SSL/TLS Settings

If your product supports HTTPS, you can configure SSL/TLS to encrypt communications with your product.

1. Access Web Config and select **Network Security Settings**.
2. Select **SSL/TLS** and select **Basic**.

You see a window like this:



3. Select one of the following options for the **Encryption Strength** setting:
   - **High** for AES256/3DES
   - **Middle** for AES256/3DES/AES128/RC4
4. Select **Enable** or **Disable** for the **Redirect HTTP to HTTPS** setting as necessary.
5. Click **Next**.

   You see a confirmation message.
6. Click **OK**.

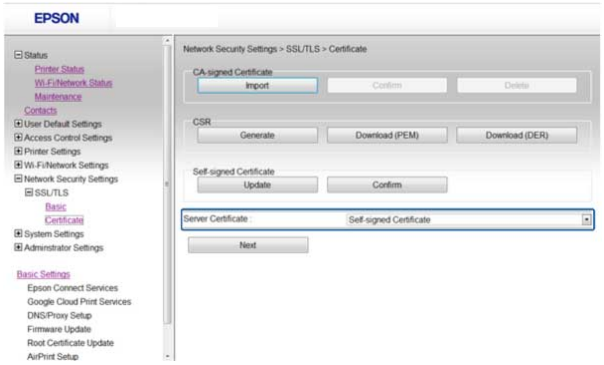
Parent topic: Configuring SSL/TLS Communication

Configuring a Server Certificate for the Product

You can configure a server certificate for your product.

1. Access Web Config and select **Network Security Settings**.
2. Select **SSL/TLS** and select **Certificate**.

You see a window like this:



3. Select one of the following options for the **Server Certificate** setting:
   - **Self-signed Certificate**: select if you have not obtained a CA-signed certificate and want the product to generate a self-signed certificate
   - **CA-signed Certificate**: select if you have obtained a CA-signed certificate
4. Click **Next**.

   You see a confirmation message.
5. Click **OK**.

Parent topic: Configuring SSL/TLS Communication

Configuring IPsec/IP Filtering

Follow the instructions in these sections to configure IPsec/IP traffic filtering using Web Config.

About IPsec/IP Filtering
Configuring Default IPsec/IP Filtering Policy
Configuring Group IPsec/IP Filtering Policies
IPsec/IP Filtering Policy Settings
IPsec/IP Filtering Configuration Examples
Configuring an IPsec/IP Filtering Certificate

Parent topic: Using Your Product on a Secure Network

About IPsec/IP Filtering

You can filter traffic to the product over the network based on IP address, service, and port by configuring a default policy that applies to every user or group connecting to the product. For control of individual users or user groups, you can configure group policies.

Note: IPsec is supported only by computers running Windows Vista or later, or Windows Server 2008 or later.

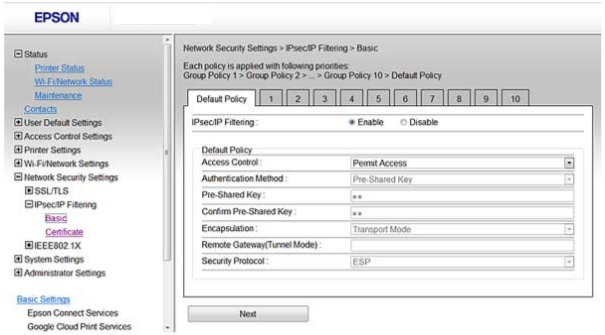
Parent topic: Configuring IPsec/IP Filtering

Configuring Default IPsec/IP Filtering Policy

You can configure the default policy for IPsec/IP traffic filtering using Web Config.

1. Access Web Config and select **Network Security Settings**.
2. Select **IPsec/IP Filtering** and select **Basic**.

   You see a window like this:



3. Select **Enable** to enable IPsec/IP filtering.
4. Select the filtering options you want to use for the default policy.
5. Click **Next**.

   You see a confirmation message.
6. Click **OK**.

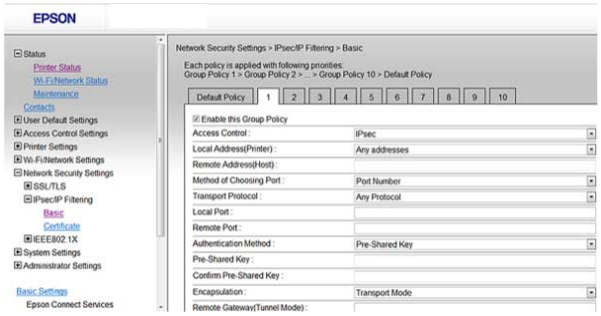
Parent topic: Configuring IPsec/IP Filtering

Configuring Group IPsec/IP Filtering Policies

You can configure group policies for IPsec/IP traffic filtering using Web Config.

1. Access Web Config and select **Network Security Settings**.
2. Select **IPsec/IP Filtering** and select **Basic**.
3. Click a tab number for the policy number you want to configure.

   You see a window like this:



4. Select the **Enable this Group Policy** checkbox.
5. Select the filtering options you want to use for this group policy.
6. Click **Next**.

   You see a confirmation message.
7. Click **OK**.
8. If you want to configure additional group policies, click the next tab number and repeat the configuration steps as necessary.

Parent topic: Configuring IPsec/IP Filtering

IPsec/IP Filtering Policy Settings

Default Policy Settings

Setting	Options/Description
Access Control	**Permit Access** to permit IP packets to pass through **Refuse Access** to prevent IP packets from passing through **IPsec** to permit IPsec packes to pass through
Authentication Method	Select an authentication method, or select **Certificate** if you have imported a CA-signed certificate
Pre-Shared Key	If necessary, enter a pre-shared key between 1 and 127 characters long
Encapsulation	If you selected **IPsec** as the **Access Control** option, select one of these encapsulation modes: **Transport Mode**, if you are using the product on the same LAN; IP packets of layer 4 or later are encrypted **Tunnel Mode**, if you are using the product on an Internet-capable network, such as IPsec-VPN; the header and data of IP packets are encrypted
Remote Gateway(Tunnel Mode)	If you selected **Tunnel Mode** as the **Encapsulation** option, enter a gateway address between 1 and 39 characters long
Security Protocol	If you selected **IPsec** as the **Access Control** option, select one of these security protocols: **ESP**, to ensure the integrity of authentication and data, and encrypt data **AH**, to ensure the integrity of authentication and data; if data encryption is prohibited, you can use IPsec

Group Policy Settings

Setting	Options/Description
Access Control	**Permit Access** to permit IP packets to pass through **Refuse Access** to prevent IP packets from passing through **IPsec** to permit IPsec packes to pass through
Local Address(Printer)	Select an IPv4 or IPv6 address that matches your network environment; if the IP address is assigned automatically, select **Use auto-obtained IPv4 address**
Remote Address(Host)	Enter the device's IP address (between 0 and 43 characters long) to control access, or leave blank to control all addresses; if the IP address is assigned automatically, such as by DHCP, the connection may be unavailable, so configure a static address instead
Method of Choosing Port	Select the method you want to used for specifiying ports
Service Name	If you selected **Service Name** as the **Method of Choosing Port** option, select a service name option here; see the next table for more information
Transport Protocol	If you selected **Port Number** as the **Method of Choosing Port** option, select one of these encapsulation modes: **Any Protocol** **TCP** **UDP** **ICMPv4** See the Group Policy Guidelines table for more information

Setting	Options/Description
Local Port	If you selected **Port Number** as the **Method of Choosing Port** option, and **TCP** or **UDP** for the **Transport Protocol** option, enter the port numbers that control receiving packets (up to 10 ports), separated by commas, for example **25,80,143,5220**; leave this setting blank to control all ports; see the next table for more information
Remote Port	If you selected **Port Number** as the **Method of Choosing Port** option, and **TCP** or **UDP** for the **Transport Protocol** option, enter the port numbers that control sending packets (up to 10 ports), separated by commas, for example **25,80,143,5220**; leave this setting blank to control all ports; see the next table for more information
Authentication Method	If you selected **IPsec** as the **Access Control** option, select an authentication method here
Pre-Shared Key	If you selected **Pre-Shared Key** as the **Authentication Method** option, enter a pre-shared key between 1 and 127 characters long here and in the **Confirm Pre-Shared Key** field
Encapsulation	If you selected **IPsec** as the **Access Control** option, select one of these encapsulation modes: **Transport Mode**, if you are using the product on the same LAN; IP packets of layer 4 or later are encrypted **Tunnel Mode**, if you are using the product on an Internet-capable network, such as IPsec-VPN; the header and data of IP packets are encrypted
Remote Gateway(Tunnel Mode)	If you selected **Tunnel Mode** as the **Encapsulation** option, enter a gateway address between 1 and 39 characters long

Setting	Options/Description
Security Protocol	If you selected **IPsec** as the **Access Control** option, select one of these security protocols: **ESP**, to ensure the integrity of authentication and data, and encrypt data **AH**, to ensure the integrity of authentication and data; if data encryption is prohibited, you can use IPsec

Group Policy Guidelines

Service name	Protocol type	Local/Remote port number	Controls these operations
ENPC	UDP	3289/Any port	Searching for a product from applications such as printer or scanner drivers, or EpsonNet Config
SNMP	UDP	161/Any port	Acquiring and configuring MIB from applications such as printer or scanner drivers, or EpsonNet Config
LPR	TCP	515/Any port	Forwarding LPR data
RAW (Port9100)	TCP	9100/any port	Forwarding RAW data
IPP/IPPS	TCP	631/Any port	Forwarding AirPrint data (IPP/IPPS printing)
WSD	TCP	Any port/5357	Controlling WSD
WS-Discovery	UDP	3702/Any port	Searching for a product from WSD
Network Scan	TCP	1865/Any port	Forwarding scan data from Document Capture Pro
Network Push Scan	TCP	Any port/2968	Acquiring job information on push scanning from Document Capture Pro
Network Push Scan Discovery	UDP	2968/Any port	Searching for a computer during push scanning from Document Capture Pro

Service name	Protocol type	Local/Remote port number	Controls these operations
FTP Data (Local)	TCP	20/Any port	Forwarding FTP printing data to FTP server
FTP Control (Local)	TCP	21/Any port	Controlling FTP printing to FTP server
FTP Data (Remote)	TCP	Any port/20	Forwarding scan data and received fax data to FTP client; controls only an FTP server that uses remote port 20
FTP Control (Remote)	TCP	Any port/21	Forwarding scan data and received fax data to FTP client
CIFS (Local)*	TCP	445/Any port	Sharing a network folder on CIFS server
CIFS (Remote)*	TCP	Any port/445	Forwarding scan data and received fax data to a folder on CIFS server
HTTP (Local)	TCP	80/Any port	Forwarding Web Config and WSD data to a HTTP or HTTPS server
HTTPS (Local)	TCP	443/Any port	
HTTP (Remote)	TCP	Any port/80	Communicating with Epson Connect, Google Cloud Printer, firmware update, and root certificate update on a HTTP or HTTPS client
HTTPS (Remote)	TCP	Any port/443	

* To control forwarding of scan and received fax data, share a network folder, or receive fax data from PC-Fax, select **Port Number** as the **Method of Choosing Port** option and specify the port numbers for CIFS and NetBIOS.

Parent topic: Configuring IPsec/IP Filtering

IPsec/IP Filtering Configuration Examples

You can configure IPsec and IP filtering in a variety of ways, as shown in the examples here.

Receiving IPsec Packets Only

Use this example only for configuring a default policy.

- **IPsec/IP Filtering**: **Enable**

- **Access Control**: **IPsec**
- **Authentication Method**: **Pre-Shared Key**
- **Pre-Shared Key**: Enter a key up to 127 characters long

Receiving Printing Data and Printer Settings

Use this example to allow communication of printing data and printer settings from specified services.

Default policy:

- **IPsec/IP Filtering**: **Enable**
- **Access Control**: **Refuse Access**

Group policy:

- **Access Control**: **Permit Access**
- **Remote Address(Host)**: Client IP address
- **Method of Choosing Port**: **Service Name**
- **Service Name**: Select **ENPc**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)**, and **RAW (Port9100)**

Receiving Access from Only a Specified Address for Product Access

In these examples, the client will be able to access and configure the product in any policy configuration.

Default policy:

- **IPsec/IP Filtering**: **Enable**
- **Access Control**: **Refuse Access**

Group policy:

- **Access Control**: **Permit Access**
- **Remote Address (Host)**: Administrator's client IP address

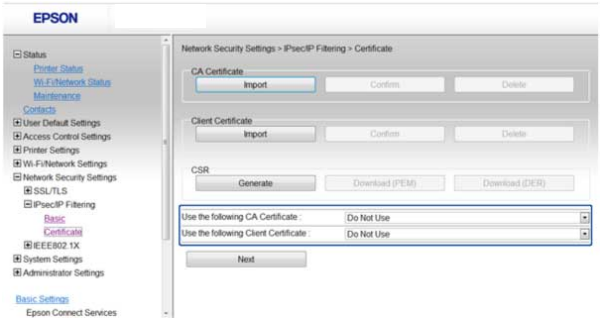
Parent topic: Configuring IPsec/IP Filtering

Configuring an IPsec/IP Filtering Certificate

You can configure a certificate for IPsec/IP traffic filtering using Web Config.

1. Access Web Config and select **Network Security Settings**.
2. Select **IPsec/IP Filtering** and select **Certificate**.

You see a window like this:



3. Select the certificate you want to use as the **Use the following CA Certificate** option.
4. Select the certificate you want to use as the **Use the following Client Certificate** option.
5. Click **Next**.

   You see a confirmation message.
6. Click **OK**.

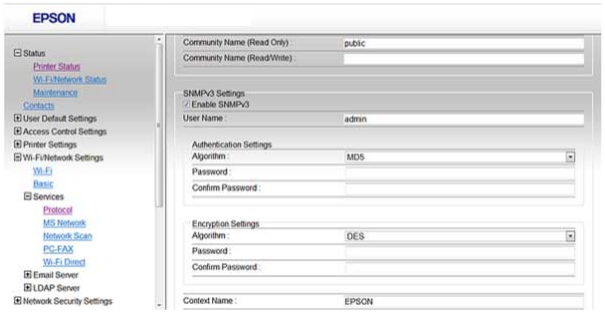
Parent topic: Configuring IPsec/IP Filtering

Configuring SNMPv3 Protocol Settings

If your product supports the SNMPv3 protocol, you can monitor and control access to your product using that protocol.

1. Access Web Config and select **Wi-Fi/Network Settings**.
2. Select **Services** and select **Protocol**.

You see a window like this:



3. Select the **Enable SNMPv3** checkbox to enable SNMPv3 settings.
4. Select the settings you want in SNMPv3 Settings section.
5. Click **Next**.

   You see a confirmation message.
6. Click **OK**.

SNMPv3 Settings

Parent topic: Using Your Product on a Secure Network

SNMPv3 Settings

You can configure these SNMPv3 settings in Web Config.

Setting	Options/Description
User Name	Enter a user name from 1 to 32 characters long in ASCII
Authentication Settings	
Algorithm	Select and algorithm for an authentication
Password	Enter a password from 8 to 32 characters long in ASCII
Confirm Password	Enter the authentication password again
Encryption Settings	

Setting	Options/Description
Algorithm	Select and algorithm for an encryption
Password	Enter a password from 8 to 32 characters long in ASCII
Confirm Password	Enter the encryption password again
Context Name	Enter a context name from 1 to 32 characters long in ASCII

Parent topic: Configuring SNMPv3 Protocol Settings

Connecting the Product to an IEEE802.1X Network

Follow the instructions in these sections to connect the product to an IEEE802.1X network using Web Config.

Configuring an IEEE802.1X Network
IEEE802.1X Network Settings
Configuring a Certificate for an IEEE802.1X Network
IEEE802.1X Network Status

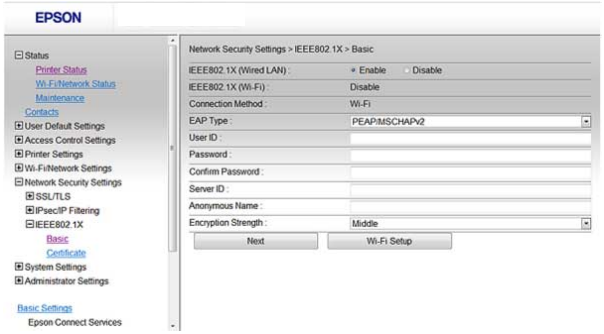
Parent topic: Using Your Product on a Secure Network

Configuring an IEEE802.1X Network

If your product supports IEEE802.1X, you can use it on a network with authentication provided by a RADIUS server with a hub as an authenticator using Web Config.

1. Access Web Config and select **Network Security Settings**.
2. Select **IEEE802.1X** and select **Basic**.

You see a window like this:



3. Select **Enable** as the **IEEE802.1X (Wired LAN)** setting.
4. To use the product on a Wi-Fi network, enable your product's Wi-Fi settings. See your product's *User's Guide* for instructions.

   The status of the connection shown in the **IEEE802.1X (Wi-Fi)** setting.

   Note: You can share the network settings for Ethernet and Wi-Fi networking.

5. Select the IEEE802.1X setting options you want to use.
6. Click **Next**.

   You see a confirmation message.
7. Click **OK**.

Parent topic: Connecting the Product to an IEEE802.1X Network

IEEE802.1X Network Settings

You can configure these IEEE802.1X network settings in Web Config.

Setting	Options/Description
Connection Method	Displays the current network connection method

Setting	Options/Description
EAP Type	Select one of these authentication methods for connections between the product and a RADIUS server: **EAP-TLS** or **PEAP-TLS**: You must obtain and import a CA-signed certificate **PEAP/MSCHAPv2**: You must configure a password
User ID	Enter an ID for authentication on a RADIUS server
Password	Enter a password for authentication of the product
Confirm Password	Enter the authentication password again
Server ID	Enter a server ID for authentication on a specified RADIUS server; server ID is verified in the subject/subjectAltName field of a server certificate sent from the RADIUS server
Anonymous Name	If you selected **PEAP-TLS** or **PEAP/MSCHAPv2** as the **Authentication Method** setting, you can configure and anonymous name instead of a user ID for phase 1 of a PEAP authentication
Encryption Strength	Select one of the following encryption strengths: **High** for AES256/3DES **Middle** for AES256/3DES/AES128/RC4

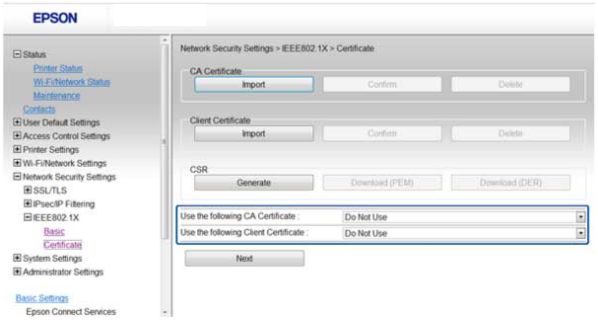
Parent topic: Connecting the Product to an IEEE802.1X Network

Configuring a Certificate for an IEEE802.1X Network

If your product supports IEEE802.1X, you can configure a certificate for the network using Web Config.

1. Access Web Config and select **Network Security Settings**.
2. Select **IEEE802.1X** and select **Certificate**.

You see a window like this:



3. Select the certificate you want to use as the **Use the following CA Certificate** option.
4. Select the certificate you want to use as the **Use the following Client Certificate** option.
5. Click **Next**.

   You see a confirmation message.
6. Click **OK**.

Parent topic: Connecting the Product to an IEEE802.1X Network

IEEE802.1X Network Status

You can check the status of the IEEE802.1X network settings by printing a status sheet from your product. See the product's *User's Guide* for instructions on printing a network status sheet.

The network status sheet displays the information in this table for IEEE802.1X networks.

Status ID	Status description
Disable	IEEE802.1X is disables
EAP Success	IEEE802.1X authentication in confirmed and the network is connected
Authenticating	IEEE802.1X authentication in progress
Config Error	Authentication has failed because the user ID was not set
Client Certificate Error	Authentication has failed because the client certificate is out of date
Timeout Error	Authentication has failed because there is no answer from the RADIUS server and/or authenticator

Status ID	Status description
User ID Error	Authentication has failed because the product's user ID and/or certificate protocol is incorrect
Server ID Error	Authentication has failed because the server ID on the server certificate and the server's ID do not match
Server Certificate Error	Authentication has failed because the server certificate is out of date or the chain of the server certificate is incorrect
CA Certificate Error	Authentication has failed because the CA certificate is incorrect, not imported, or out of date
EAP Failure	Authentication has failed because the client certificate is incorrect (EAP-TLS or PEAP-TLS), or the user ID or password is incorrect (PEAP/MSCHAPv2)

Parent topic: Connecting the Product to an IEEE802.1X Network

Using a Digital Certificate

Follow the instructions in these sections to configure and use digital certificates using Web Config.

About Digital Certification
Obtaining and Importing a CA-signed Certificate
CSR Setup Settings
CSR Import Settings
Deleting a CA-signed Certificate
Updating a Self-signed Certificate

Parent topic: Using Your Product on a Secure Network

About Digital Certification

You can configure the following digital certificates for your network using Web Config:

CA-signed Certificate
You can insure secure communications using a CA-signed certificate for each security feature. The certificates must be signed by and obtained from a CA (Certificate Authority).

Self-signed Certificate
A self-signed certificate is issued and signed by the product itself. You can use the certificate for only SSL/TLS communication, however security is unreliable and you may see a security alert in the browser during use.

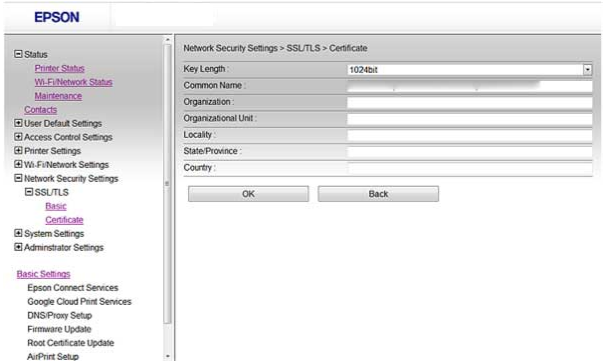
Parent topic: Using a Digital Certificate

Obtaining and Importing a CA-signed Certificate

You can obtain a CA-signed certificate by creating a CSR (Certificate Signing Request) using Web Config and submitting it to a certificate authority. The CSR created in Web Config is in PEM/DER format. You can import one CSR created from Web Config at a time.

1. Access Web Config and select **Network Security Settings**.
2. Select one of the following network security options:
   - **SSL/TLS**
   - **IPsec/IP Filtering**
   - **IEEE802.1X**
3. Select **Certificate**.
4. In the CSR section, select **Generate**.

   You see a window like this:



5. Select the CSR setting options you want to use.
6. Click **OK**.

   You see a completion message.
7. Select **Network Security Settings**, select your network security option, and select **Certificate** again.

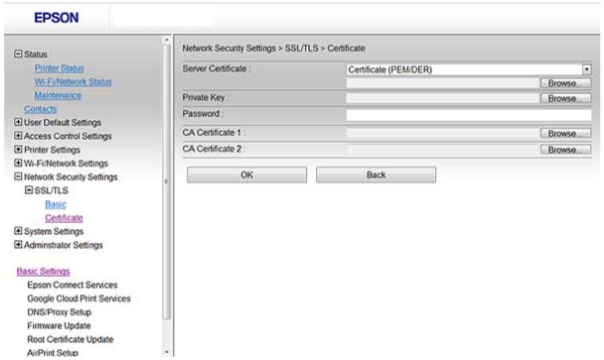
8. In the CSR section, click the **Download** option that matches the format specified by your certificate authority to download the CSR.

   Caution: Do not generate another CSR or you may not be able to import a CA-signed certificate.

9. Submit the CSR to the certificate authority following the format guidelines provided by that authority.
10. Save the issued CA-signed certificate to a computer connected to the product.

    Before proceeding, make sure the time and date settings are correct on your product. See the product's *User's Guide* for instructions.
11. Select **Network Security Settings**, select your network security option, and select **Certificate** again.
12. In the CA Certificate section, click **Import**.

    You see a window like this:



13. Select the format of the certificate as the **Server Certificate** settings.
14. Select the certificate import settings as necessary for the format and the source from which you obtained it.
15. Click **OK**.

    You see a confirmation message.
16. Click **Confirm** to verify the certificate information.

Parent topic: Using a Digital Certificate

CSR Setup Settings

You can select these settings when setting up a CSR in Web Config.

Note: The available key length and abbreviations vary by certificate authority, so follow the rules of that authority when entering information in the CSR.

Setting	Options/Description
Key Length	Select a key length for the CSR
Common Name	Enter a name or static IP address from 1 to 128 characters long; for example, **Reception printer** or **https://10.152.12.225**
Organization, **Organizational Unit**, **Locality**, **State**, and **Province**	Enter information in each field as necessary, from 0 to 64 characters long in ASCII; separate any multiple names with commas
Country	Enter a two-digit country code number as specified by the ISO-3166 standard

Parent topic: Using a Digital Certificate

CSR Import Settings

You can configure these settings when importing a CSR in Web Config.

Note: The import setting requirements vary by certificate format and how you obtained the certificate.

Certificate format	Setting descriptions
PEM/DER format obtained from Web Config	**Private Key**: Do not configure because the product contains a private key **Password**: Do not configure **CA Certificate 1/CA Certificate 2**: Optional
PEM/DER format obtained from a computer	**Private Key**: Configure a private key **Password**: Do not configure **CA Certificate 1/CA Certificate 2**: Optional

Certificate format	Setting descriptions
PKCS#12 format obtained from a computer	**Private Key**: Do not configure **Password**: Optional **CA Certificate 1/CA Certificate 2**: Do not configure

Parent topic: Using a Digital Certificate

Deleting a CA-signed Certificate

You can delete an imported CA-signed certificate with Web Config when the certificate expires or if you have no more need for an encrypted connection.

Note: If you obtained a CA-signed certificate from Web Config, you cannot import a deleted certificate; you must obtain and import a new certificate.

1. Access Web Config and select **Network Security Settings**.
2. Select **SSL/TLS** and select **Certificate**.
3. Click **Delete**.

   You see a completion message.
4. Click **OK**.

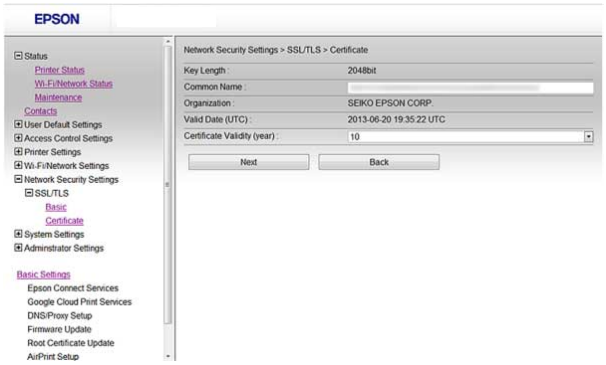
Parent topic: Using a Digital Certificate

Updating a Self-signed Certificate

If your product supports the HTTPS server feature, you can update a self-signed certificate using Web Config.

1. Access Web Config and select **Network Security Settings**, select **SSL/TLS**, and select **Certificate**.
2. Click **Update**.

You see a window like this:



3. Enter an identifier for your product from 1 to 128 characters long in the **Common Name** field.
4. Select a validity period for the certificate as the **Certificate Validity (year)** setting.
5. Click **Next**.

   You see a completion message.
6. Click **OK**.
7. Click **Confirm** to verify the certificate information.

Parent topic: Using a Digital Certificate

Using an LDAP Server

Follow the instructions in these sections to use an LDAP server to provide fax and email destination information using Web Config.

Configuring the LDAP Server and Selecting Search Settings
LDAP Server Settings
LDAP Search Settings
Checking the LDAP Server Connection
LDAP Connection Report Messages

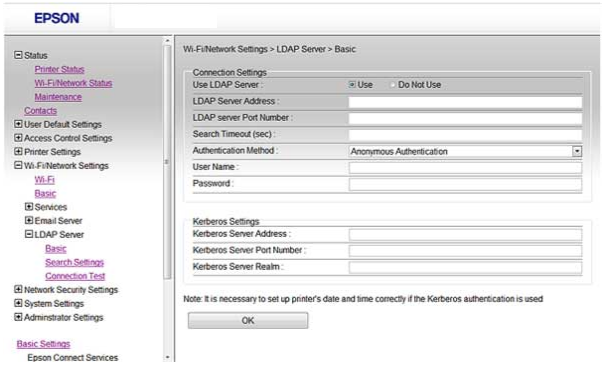
Parent topic: Using Your Product on a Secure Network

Configuring the LDAP Server and Selecting Search Settings

You can configure the LDAP server and select search settings for it using Web Config.

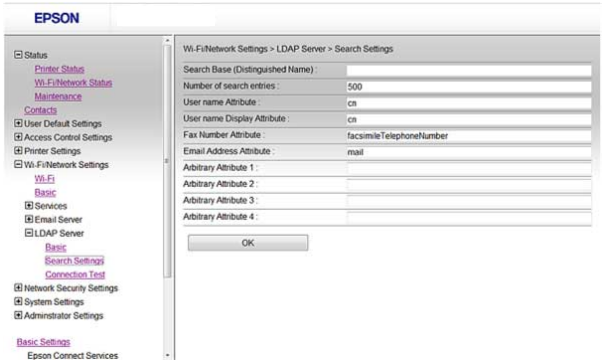
1. Access Web Config and select **Wi-Fi/Network Settings**.
2. Select **LDAP Server** and select **Basic**.

   You see a window like this:



3. Select **Use** as the **Use LDAP Server** setting.
4. Select the LDAP server settings.
5. Click **OK**.
6. Select **Wi-Fi/Network Settings** and select **LDAP Server** again.
7. Select **Search Settings**.

   You see a window like this:



8. Select the LDAP search settings you want to use.
9. Click **OK**.

Parent topic: Using an LDAP Server

LDAP Server Settings

You can configure these LDAP server settings in Web Config.

Setting	Options/Description
LDAP Server Address	Enter the address of the LDAP server as necessary, depending on the format of the server: • IPv4 or IPv6 format: Enter from 1 to 255 characters • FQDN format: Enter from 1 to 255 alphanumeric characters in ASCII; you can use "-", except at the beginning or end of the address
LDAP server Port Number	Enter an LDAP server port number between 1 and 65535
Search Timeout (sec)	Enter a search time interval before timeout from between 5 and 300 seconds
Authentication Method	Select one of the available authentication methods listed
User Name	Enter a user name for the LDAP server from 0 to 128 characters long in Unicode (UTF-8); do not use control characters such as 0x00-0x1F or OX7F (not available when you selected **Anonymous Authentication** as the **Authentication Method** option)
Password	Enter a password from 0 to 128 characters long in Unicode (UTF-8) for LDAP server authentication; do not use control characters such as 0x00-0x1F or OX7F (not available when you selected **Anonymous Authentication** as the **Authentication Method** option)
Kerberos Server Address	If you selected **Kerberos Authentication** as the **Authentication Method** option, enter the Kerberos server port number between 1 and 65535
Kerberos Server Port Number	If you selected **Kerberos Authentication** as the **Authentication Method** option, enter

Setting	Options/Description
Kerberos Server Realm	If you selected **Kerberos Authentication** as the **Authentication Method** option, enter the realm of Kerberos authentication from 0 to 255 characters long in ASCII

Parent topic: Using an LDAP Server

LDAP Search Settings

You can configure these LDAP search settings in Web Config.

Setting	Options/Description
Search Base (Distinguished Name)	Leave blank or search for an arbitrary domain name on the LDAP server using 1 to 128 characters (Unicode (UTF-8)
Number of search entries	Specify the maximum number of search entries before an error message appears, from 1 to 500
User name Attribute	Enter the attribute name to display when searching for users names from 1 to 255 characters long in Unicode (UTF-8); the first character must be a-z, or A-Z
User name Display Attribute	Enter the attribute name to display as the user name from 0 to 255 characters long in Unicode (UTF-8); the first character must be a-z, or A-Z
Fax Number Attribute	Enter the attribute name to display when searching for fax numbers from 1 to 255 characters long using A-Z, a-z, 0-9, and "-" in Unicode (UTF-8); the first character must be a-z, or A-Z
Email Address Attribute	Leave blank or enter the attribute name to display when searching for email addresses from 0 to 255 characters long in Unicode (UTF-8); the first character must be a-z, or A-Z
Arbitrary Attribute 1 through **Arbitrary Attribute 4**	Leave blank or specify other arbitrary attributes to search for from 1 to 255 characters long in Unicode (UTF-8); the first character must be a-z, or A-Z

Parent topic: Using an LDAP Server

Checking the LDAP Server Connection

You can test the LDAP server connection and view a connection report using Web Config.

1. Access Web Config and select **Wi-Fi/Network Settings**.
2. Select **LDAP Server** and select **Connection Test**.
3. Click **Start**.

   Web Config tests the connection and displays the connection report when it is finished.

Parent topic: Using an LDAP Server

LDAP Connection Report Messages

You can review the connection report messages to diagnose LDAP connection problems in Web Config.

Message	Description
Connection test was successful.	Connection to the server is successful
Connection test failed. Check the settings.	One of the following has occurred: • The LDAP server address or port number is incorrect • A timeout has occurred • You selected **Do Not Use** as the **Use LDAP Server** setting • If you selected **Kerberos Authentication** as the **Authentication Method** setting, the Kerberos server settings are incorrect
Connection test failed. Check the date and time on your printer or server.	Connection has failed because the time settings for the product and the LDAP server do not match
Authentication failed. Check the settings.	Authentication has failed because the User Name and Password settings are incorrect or, If you selected **Kerberos Authentication** as the **Authentication Method** setting, the time and date are not configured correctly
Cannot access the printer until processing is complete.	The product is busy.

Parent topic: Using an LDAP Server

Using an Email Server

Follow the instructions in these sections to use an email server to send scan and fax data by email, or use email notification using Web Config.

Configuring an Email Server
Email Server Settings
Checking the Email Server Connection
Email Server Connection Report Messages
Configuring Email Notification

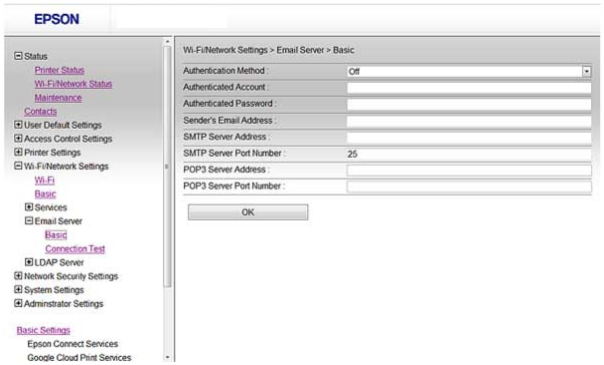
Parent topic: Using Your Product on a Secure Network

Configuring an Email Server

You can configure an email server using Web Config.

1. Access Web Config and select **Wi-Fi/Network Settings**.
2. Select **Email Server** and select **Basic**.

   You see a window like this:



3. Select the email server settings.
4. Click **OK**.

Parent topic: Using an Email Server

Email Server Settings

You can configure these email server settings in Web Config.

Setting	Options/Description
Authentication Method	Select the authentication method that matches your email server

Setting	Options/Description
Authenticated Account	Enter the authenticated account name from 0 to 30 characters long in ASCII
Authenticated Password	Enter the authenticated password from 0 to 20 characters long in ASCII using A-Z, a-z, 0-9, and these characters: ! # $ % ' * + - . / = ? ^ _ { ! } ~ @
Sender's Email Address	Enter the sender's email address from 0 to 255 characters long in ASCII; do not use a period (.) as the first character or use these characters: ( ) < > [ ] ;
SMTP Server Address	Enter the SMTP server address from 0 to 255 characters long using A-Z, a-z, 0-9, and "-" in IPv4 or FQDN format
SMTP Server Port Number	Enter the SMTP server port number between 1 and 65535
POP3 Server Address	Enter the POP server address from 0 to 255 characters long using A-Z, a-z, 0-9, and "-" in IPv4 or FQDN format
POP3 Server Port Number	Enter the POP server port number between 1 and 65535

Parent topic: Using an Email Server

Checking the Email Server Connection

You can test the email server connection and view a connection report using Web Config.

1. Access Web Config and select **Wi-Fi/Network Settings**.
2. Select **Email Server** and select **Connection Test**.
3. Click **Start**.

   Web Config tests the connection and displays the connection report when it is finished.

Parent topic: Using an Email Server

Email Server Connection Report Messages

You can review the connection report messages to diagnose email server connection problems in Web Config.

Message	Description
Connection test was successful.	Connection to the server is successful

Message	Description
Connection test failed. Check the settings.	One of the following has occurred: • The email server address or port number is incorrect • A timeout has occurred
Cannot access the printer until processing is complete.	The product is busy.

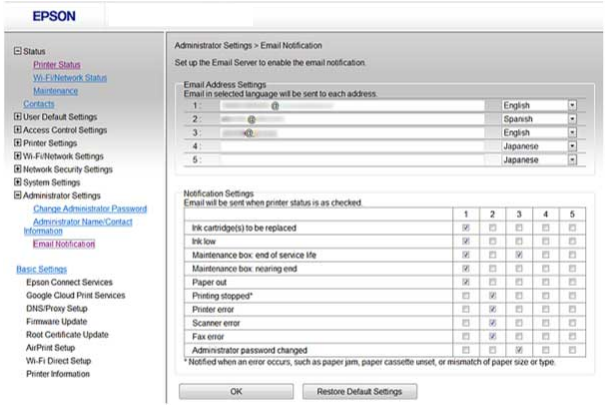
Parent topic: Using an Email Server

Configuring Email Notification

You can configure email notifications using Web Config so you can receive alerts by email when certain events occur on the product, such as running out of paper. You can register up to 5 email addresses and select the events for which you want to be notified.

1. Access Web Config and select **Adminstrator Settings**.
2. Select **Email Notification**.

   You see a window like this:



3. Enter an email address in the **1** field.
4. Select the language in which you want to receive the email notifications from the drop-down menu for the first email address.
5. Enter additional email addresses in fields **2** through **5** as necessary, and select a language for each.

6. Select the checkboxes to indicate the events for which you want to receive email notifications.
7. Click **OK**.

Parent topic: Using an Email Server

Using EpsonNet Config Network Configuration Software

Follow the instructions in these sections to configure your product's administrator network settings using the EpsonNet Config software.

With Windows, you can configure network settings in a batch operation. See the EpsonNet Config help utility for instructions.

Note: Before you can configure system administration settings, connect the product to a network. See the product's *Start Here* sheet and *User's Guide* for instructions.

Installing EpsonNet Config
Configuring a Product IP Address Using EpsonNet Config - Ethernet
Configuring a Product IP Address Using EpsonNet Config - WiFi

Installing EpsonNet Config

To install EpsonNet Config, download the software from the product's support page at epson.com/support and follow the on-screen instructions.

Parent topic: Using EpsonNet Config Network Configuration Software

Configuring a Product IP Address Using EpsonNet Config - Ethernet

You can configure the product's IP address using EpsonNet Config.

1. Turn on the product.
2. Connect the product to a network using an Ethernet cable.
3. Do one of the following to start EpsonNet Config:
   - **Windows 8.x**: Navigate to the **Apps** screen and select **EpsonNet Config** under **EpsonNet**.
   - **Windows (other versions)**: Click or **Start**, and select **All Programs** or **Programs**. Select **EpsonNet** and click **EpsonNet Config**.
   - **OS X**: Open the **Applications** folder, open the **Epson Software** folder, select EpsonNet, select EpsonNet Config, and double-click the **EpsonNet Config** icon.

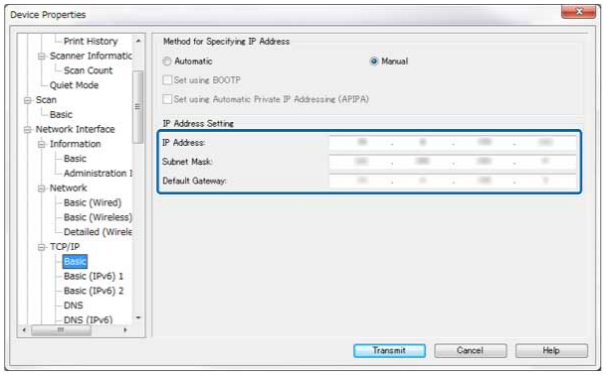
   After a few moments, the program displays the connected products.

4. Double-click the product you are configuring.

   Note: If several products of the same model are connected, you can identify them by their MAC address.

5. From the menu on the left, select **Network Interface**, select **TCP/IP**, and select **Basic**.

   You see a window like this:



6. Enter the product's **IP address**, **Subnet Mask**, and **Default Gateway** settings in the fields provided.

   Note: To connect the product to a secure network, enter a static IP address. You can also configure the DNS settings by selecting **DNS**, and enter proxy settings by selecting **Internet** from the **TCP/IP** menu.

7. Select **Transmit**.

Parent topic: Using EpsonNet Config Network Configuration Software

Configuring a Product IP Address Using EpsonNet Config - WiFi

You can configure the product's IP address using EpsonNet Config.

1. Turn on the product.
2. Connect the product to a network using an Ethernet cable.
3. Do one of the following to start EpsonNet Config:
   - **Windows 8.x**: Navigate to the **Apps** screen and select **EpsonNet Config** under **EpsonNet**.

- **Windows (other versions)**: Click or **Start**, and select **All Programs** or **Programs**. Select **EpsonNet** and click **EpsonNet Config**.
- **OS X**: Open the **Applications** folder, open the **Epson Software** folder, select EpsonNet, select EpsonNet Config, and double-click the **EpsonNet Config** icon.

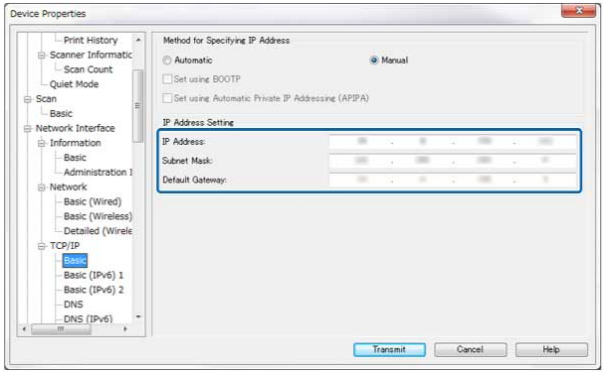
After a few moments, the program displays the connected products.

4. Double-click the product you are configuring.

   Note: If several products of the same model are connected, you can identify them by their MAC address.

5. From the menu on the left, select **Network Interface**, select **TCP/IP**, and select **Basic**.

   You see a window like this:

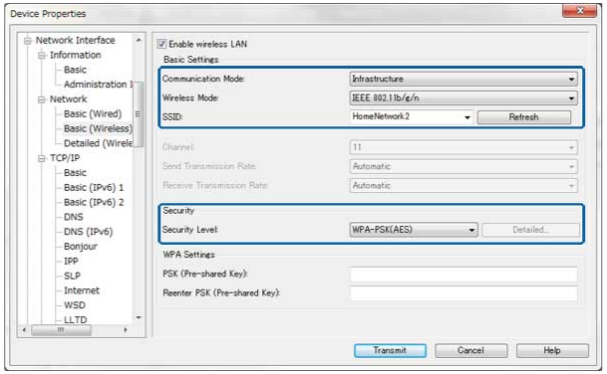


6. Enter the product's **IP address**, **Subnet Mask**, and **Default Gateway** settings in the fields provided.

   Note: To connect the product to a secure network, enter a static IP address. You can also configure the DNS settings by selecting **DNS**, and enter proxy settings by selecting **Internet** from the **TCP/IP** menu.

7. From the menu on the left, select **Network Interface**, select **Network**, and select **Basic (Wireless)**.

You see a window like this:



8. Enter the **Communication Mode**, **Wireless Mode**, **SSID**, and **Security Level** settings for the Wi-Fi network as necessary.
9. Select **Transmit**.
10. Confirm the Wi-Fi connection to the product and disconnect the Ethernet cable from the product.

Parent topic: Using EpsonNet Config Network Configuration Software

Solving Problems

Check these sections for solutions to problems you may have with the network configuration software.

Solving Network Software Usage Problems
Solving Network Security Problems
Solving Digital Certificate Problems
Where to Get Help

Solving Network Software Usage Problems

Check these sections if you have problems using the network software.

Cannot Find Access Web Config
The "Out of Date" Message Appears
"The name of the security certificate does not match" Message Appears
Model Name or IP Address Not Displayed in EpsonNet Config

Parent topic: Solving Problems

Cannot Find Access Web Config

If you cannot access Web Config on your product, try these solutions:

- Make sure your product is turned on and connected to your network using the correct IP address. Verify connection using your product control panel or print a network status sheet. See your product's *User's Guide* for instructions.
- If you selected **High** as the **Encryption Strength** setting in Web Config, your browser must support AES (256-bit) or 3DES (168-bit) encryption. Check your browser's encryption support or select a different **Encryption Strength** option.
- If you are using a proxy server with your product, configure the browser's proxy settings as follows:
  - **Windows**: Select **Control Panel** > **Network and Internet** > **Internet Options** > **Connections** > **LAN settings** > **Proxy server**. Select the setting that does not use the proxy server for local addresses.
  - **OS X**: Select **System Preferences** > **Network** > **Advanced** > **Proxies**. Register the local address under **Bypass proxy settings for these Hosts & Domains**. For example, 192.168.1.*: Local address 192.168.1.XXX, subnet mask 255.255.255.0.

Parent topic: Solving Network Software Usage Problems

The "Out of Date" Message Appears

If the "Out of Date" message appears when you are accessing Web Config using SSL communication (HTTPS), the certificate is out of date. Make sure that the product date and time are configured correctly, and obtain a new certificate.

Parent topic: Solving Network Software Usage Problems

"The name of the security certificate does not match" Message Appears

If a message beginning with "The name of the security certificate does not match . . ." appears when you are accessing Web Config using SSL communication (HTTPS), the product's IP address on the CSR or self-signed certificate does not match what you entered in the browser. Change the IP address you entered for the **Common Name** setting, and obtain and import a certificate again, or change the product name.

Parent topic: Solving Network Software Usage Problems

Model Name or IP Address Not Displayed in EpsonNet Config

If the product model name and/or IP address is not displayed in EpsonNet Config, try these solutions:

- If you selected to block, cancel, or shut down option on a Windows security or firewall screen, the IP address and model name cannot display in EpsonNet Config. Register EpsonNet config as an exception in your firewall or security software, or close the security software and try running EpsonNet Config again.
- The operation may have timed out. Select **Tools**, select **Options**, select **Timeout**, and increase the time option for the **Communication Error** setting. This may cause EpsonNet Config to run slower, however.

Parent topic: Solving Network Software Usage Problems

Solving Network Security Problems

Check these sections if you have problems using the network security features.

Pre-Shared Key was Forgotten
Cannot Communicate with the Product Using IPsec Communication
Communication was Working, but Stopped
Cannot Create the Secure IPP Printing Port
Cannot Access the Product After Configuring IEEE802.1X

Parent topic: Solving Problems

Pre-Shared Key was Forgotten

If you forget a pre-shared key, change the key using Web Config for the default or group policy.

Parent topic: Solving Network Security Problems

Cannot Communicate with the Product Using IPsec Communication

Make sure your computer is using one of these supported algorithms for communicating with the product:

Security method	Supported algorithms
Consistency Algorithm	AES-CBC 128
	AES-CBC 192
	AES-CBC 256
	3DES-CBC
	DES-CBC
Hash Algorithm	SHA-1
	SHA2-256
	SHA2-384
	SHA2-512
	MD5
Algorithm Compatible with a key	Diffie-Hellman Group2
	Diffie-Hellman Group1, Diffie-Hellman Group14, Elliptic Curve Diffie-Hellman P-256, Elliptic Curve Diffie-Hellman P-384; available method may vary by model

Parent topic: Solving Network Security Problems

Communication was Working, but Stopped

If network communication was working, but suddenly stopped, the product's and/or computer's IP address may have changed or is invalid. Try these solutions:

- Disable IPsec using the product control panel.

- If DHCP is out of date, or the IPv6 address is out of date or was not obtained, you may not be able to find the IP address registered in Web Config.
- If that does not solve the problem, enter a static IP address using Web Config.

Parent topic: Solving Network Security Problems

Cannot Create the Secure IPP Printing Port

If you cannot create the secure IPP printing port, try these solutions:

- Make sure you specified the correct server certificate for SSL/TLS communication using Web Config.
- If you are using a CA certificate, make sure it is imported to the computer that is accessing the printer.

Parent topic: Solving Network Security Problems

Cannot Access the Product After Configuring IEEE802.1X

If you cannot access the product after configuring it for IEEE802.1X, disable IEEE802.1X and Wi-Fi using the product control panel. Then connect the product and a computer, and configure IEEE802.1X using Web Config again.

Parent topic: Solving Network Security Problems

Solving Digital Certificate Problems

Check these sections if you have problems using a digital certificate.

Digital Certificate Warning Messages
Cannot Import a Digital Certificate
Cannot Update a Certificate or Create a CSR
Deleted a CA-signed Certificate

Parent topic: Solving Problems

Digital Certificate Warning Messages

If you see a warning message when using a digital certificate, check for solutions in this table.

Message	Solution
Enter a Server Certificate.	Select a certificate file and click **Import**.
CA Certificate 1 is not entered.	Import CA certificate 1 before importing additional certificates.

Message	Solution
Invalid value below.	Remove any unsupported characters in the file path and password.
Invalid date and time.	Set the date and time on the product using Web Config, EpsonNet Config, or the product control panel.
Invalid password	Enter the password that matches the password set for the CA certificate.
Invalid file	Try the following: • Import only certificate files in X509 format sent by a trusted certificate authority. • Make sure the file size is 5KB or less and is not corrupted or fabricated. • Make sure the chain in the certificate is valid; check the certificate authority's website.
Cannot use the Server Certificates that include more than three CA certificates.	Import certificate files in PKCS#12 format that contains one or two CA certificates, or convert each certificate to PRM format and import them again.
The certificate has expired. Check if the certificate is valid, or check the date and time on your printer.	Make sure the product time and date are set correctly and, if the certificate is out of date, obtain and import a new certificate.
Private key is required.	Do one of the following to pair a private key with the certificate: • For PEM/DER format certificates obtained from a CSR using a computer, specify the private key file. • For PKCS#12 format certificates obtained from a CSR using a computer, create a file containing the private key. If you re-imported a PEM/DER format certificate obtained from a CSR using Web Config, you can only import it once. You must obtain and import a new certificate.

Message	Solution
Setup failed.	Make sure the computer and product are connected, and the certificate file is not corrupted, then import the certificate file again.

Parent topic: Solving Digital Certificate Problems

Cannot Import a Digital Certificate

If you cannot import a digital certificate, try these solutions:

- Make sure the CA-signed certificate and the CSR have the same information. If they do not match, import the certificate to a device that matches the information or use the CSR to obtain the CA-signed certificate again.
- Make sure the CA-signed certificate file size is 5KB or less.
- Make sure you are entering the correct password.

Parent topic: Solving Digital Certificate Problems

Cannot Update a Certificate or Create a CSR

If you cannot update a self-signed certificate or create a CSR for a CA-signed certificate, try these solutions:

- Make sure that you entered a **Common Name** setting in Web Config.
- Make sure the **Common Name** setting does not contain unsupported characters or is divided by a comma. Correct the setting and update the certificate again.

Parent topic: Solving Digital Certificate Problems

Deleted a CA-signed Certificate

If you accidentally deleted a CA-signed certificate, try these solutions:

- If you retained a backup file, import the CA-signed certificate again.
- If you obtained the certificate using a CSR created in Web Config, you cannot import a deleted certificate. Create a new CSR and obtain a new certificate.

Parent topic: Solving Digital Certificate Problems

Where to Get Help

If you need to contact Epson for technical support services, use the following support options.

Internet Support

Visit Epson's support website at epson.com/support (U.S.) or epson.ca/support (Canada) for solutions to common problems. You can download drivers and documentation, get FAQs and troubleshooting advice, or e-mail Epson with your questions.

Speak to a Support Representative

Before you call Epson for support, please have the following information ready:

- Product name
- Product serial number (located on a label on the product)
- Proof of purchase (such as a store receipt) and date of purchase
- Computer configuration
- Description of the problem

Then see your product's *User's Guide* for contact information.

Purchase Supplies and Accessories

You can purchase genuine Epson ink and paper at Epson Supplies Central at epson.com/ink3 (U.S. sales) or epson.ca (Canadian sales). You can also purchase supplies from an Epson authorized reseller. To find the nearest one, call 800-GO-EPSON (800-463-7766).

Parent topic: Solving Problems

Notices

Check these sections for important notices.

Trademarks
Copyright Notice

Trademarks

EPSON® is a registered trademark abd EPSON Exceed Your Vision is a registered logomark of Seiko Epson Corporation.

OS X is a trademark of Apple Inc., registered in the U.S. and other countries.

General Notice: Other product names used herein are for identification purposes only and may be trademarks of their respective owners. Epson disclaims any and all rights in those marks.

Parent topic: Notices

Copyright Notice

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Seiko Epson Corporation. The information contained herein is designed only for use with this Epson product. Epson is not responsible for any use of this information as applied to other products.

Neither Seiko Epson Corporation nor its affiliates shall be liable to the purchaser of this product or third parties for damages, losses, costs, or expenses incurred by purchaser or third parties as a result of: accident, misuse, or abuse of this product or unauthorized modifications, repairs, or alterations to this product, or (excluding the U.S.) failure to strictly comply with Seiko Epson Corporation's operating and maintenance instructions.

Seiko Epson Corporation shall not be liable for any damages or problems arising from the use of any options or any consumable products other than those designated as Original Epson Products or Epson Approved Products by Seiko Epson Corporation.

Seiko Epson Corporation shall not be held liable for any damage resulting from electromagnetic interference that occurs from the use of any interface cables other than those designated as Epson approved Products by Seiko Epson Corporation.

This information is subject to change without notice.

Copyright Attribution

Parent topic: Notices

Copyright Attribution

© 2014 Epson America, Inc.

8/14

CPD-41038R1

Parent topic: Copyright Notice